DETAILED ACTION

- A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.1 14, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.1 14. Applicant's submission filed on 12/17/2008 has been entered.
- Claims 1-8, 11-23, 26-38, 41-45 are presented for further examination.

Response to Arguments

Applicant's arguments with respect to claims 1-8, 11-23, 26-38, 41-45 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 16-23, 26-38, 41-45 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 16-23, 26-30 are rejected under 35 USC 101 because according to Claim 31, that an “Apparatus” only contains sets of "instructions" (i.e., software instructions) and does not embody any functional hardware structure. Therefore, an “apparatus" that contains sets of

instructions is considered as software per se, and does not fall into any one of the categories of statutory subject matter.

Claims 31-38, 41-45 are rejected under 35 USC 101 because according to page 56 of the specification that computer program product in a computer-readable medium such as "communications links" which does not does not fall into any one of the categories of statutory subject matter.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-8, 11-23, 26-38, 41-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yavatkar et al hereinafter Yavatkar (US 6,735,702) in view of Aoki et al hereinafter Aoki (US 6,757,255) in further view of Phaal (US 2005/0190695).

1. Referring to Claim 1, Yavatkar discloses a method for monitoring network packets transmitted within a distributed data processing system, the method comprising: monitoring multiple sources of network packets within the distributed data processing system (refer to Col 4, Lines 1–3, Col 15, Lines 65-66); identifying a source of network packets (refer to abstracts) by deploying distributed packet snoopers (SNMP is used by the agent to snoop the information, refer to Col 11, Lines 50-55) from a packet usage manager to monitor the multiple sources of

network packets receiving packet filtering parameters at each of the deployed distributed packet snoopers (refer to Col 5, Lines 36-45 and Col 15, Lines 35-40), and matching packet filtering parameters against transmitted packets (refer to Col 15, lines 16-45), wherein the packet filtering parameters specify at least a packet type and a packet size of a packet (id type of traffic include the packet type and packet size, refer to Col 16, lines 1-17); and alerting a system administrator to the identified source of network packets by returning packet usage events to the packet usage manager in response to a determination that a packet surpassed a limitation specified by the packet filtering parameters (refer to Col 16, Lines 17-21 and Col 17, Lines 25-30 and Col 18, Lines 10-18 and Col 19, Lines 1-7).

Although Yavatkar disclosed the invention substantially as claimed, Yavatkar did not explicitly disclosing " identifying a source of network packets as generating network packets having packet size characteristics directly related to packet size of individual packets of the network packets that satisfy one or more predetermined conditions."

Aoki, in analogous art, disclosing "identifying a source of network packets as generating network packets having packet size characteristics directly related to packet size of individual packets of the network packets that satisfy one or more predetermined conditions (refer to Col 7, Lines 25-65)"

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine Yavatkar and Aoki because Aoki's teaching of "identifying a source of network packets as generating network packets having packet size characteristics directly related to packet size of individual packets of the network packets that satisfy one or more predetermined conditions" would improve the Yavatkar's system performance by efficiently

calculate the effective bandwidth during the time when the network is congested (also supported by Phaal, refer to par 0031 and 0069).

2. Referring to Claim 2, Yavatkar, Aoki and Phaal disclosed the method of claim 1. Although Yavatkar disclosed the invention substantially as claimed, Yavatkar did not explicitly disclosing "wherein a predetermined condition of the one or more predetermined conditions is a packet size less than a predetermined packet size threshold value."

Aoki, in analogous art, disclosing "wherein a predetermined condition of the one or more predetermined conditions is a packet size less than a predetermined packet size threshold value (refer to Col 7, Lines 25-65)"

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine Yavatkar and Aoki because Aoki's teaching of "wherein a predetermined condition of the one or more predetermined conditions is a packet size less than a predetermined packet size threshold value" would improve the Yavatkar's system performance by efficiently calculate the effective bandwidth during the time when the network is congested (also supported by Phaal, refer to par 0031 and 0069).

3. Referring to Claim 3, Yavatkar, Aoki and Phaal disclosed the method of claim 1. Although Yavatkar disclosed the invention substantially as claimed, Yavatkar did not explicitly disclosing "wherein a predetermined condition of the one or more predetermined conditions is a computed percentage value of an actual packet payload size in comparison to a maximum available packet payload size."

Aoki, in analogous art, disclosing "wherein a predetermined condition of the one or more predetermined conditions is a computed percentage value of an actual packet payload size in comparison to a maximum available packet payload size (refer to Col 11, Lines 35-60)"

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine Yavatkar and Aoki because Aoki's teaching of "wherein a predetermined condition of the one or more predetermined conditions is a computed percentage value of an actual packet payload size in comparison to a maximum available packet payload size" would improve the Yavatkar's system performance by efficiently calculate the effective bandwidth during the time when the network is congested (also supported by Phaal, refer to par 0031 and 0069).

4. Referring to Claim 4, Yavatkar, Aoki and Phaal disclosed the method of claim 1, Yovatkar disclosing wherein a predetermined condition of the one or more predetermined conditions is a count of a number of packets, where the number packets is the number of individual packets having a packet size less than a predetermined packet size threshold value, that exceed a predetermined maximum count threshold value (capable to detect the large amount of packets, refer to Col 13, Lines 20-30 and Col 16, Lines 1-18)

5. Referring to Claim 5, Yavatkar, Aoki and Phaal disclosed the method of claim 1. Yavatkar further discloses wherein a predetermined condition of the one or more predetermined conditions is a computed percentage value of a number of packets, where the number of packets is the number of individual packets having a packet size less than a predetermined packet size

threshold value, in comparison to a number of packets from the identified source of network packets (refer to Col 16, Lines 1-18).

6. Referring to Claim 6, Yavatkar, Aoki and Phaal disclosed the method of claim 1. Yavatkar further disclosing: in response to a request of the system administrator, halting execution of the identified source (refer to Col 9, lines 25-30).

7. Referring to Claim 7, Yavatkar, Aoki and Phaal disclosed the method of claim 1, Yavatkar further disclosing in response to a request of the system administrator, pausing execution of the identified source (refer to Col 9, Lines 25-30).

8. Referring to Claim 8, Yavatkar, Aoki and Phaal disclosed the method of claim 1. Yavatkar further disclosing initiating a packet snooping session (refer to Col 13, Lines 55-67).

9. Referring to Claim 11 Yavatkar, Aoki and Phaal disclosed the method of claim 1. Yavatkar further disclosing receiving a request for an action at a target resource within the distributed data processing system (refer to Col 7, Lines 42-60), wherein completion of the action depends upon operations of a set of resources along a logical route through the distributed data processing system, wherein the request for the action at the target resource is associated with a user or an application (refer to Fig 3).

10. Referring to Claim 12. Yavatkar, Aoki and Phaal disclosed the method of claim 11. Yavatkar further disclosing deriving one of the packet filtering parameters from an application or a user associated with the request for the action at the target resource (refer to Col 3, Lines 25-60).

11. Referring to Claim 13, Yavatkar, Aoki and Phaal disclosed the method of claim 11. Yavatkar further disclosing selecting by the system administrator one of the packet filtering parameters by choosing among a plurality of active applications or users within the data processing system (SNMP protocol providing the ability to detect the active application/users, refer to Col 11, Lines 50-55).

12. Referring to Claim 14, Yavatkar, Aoki and Phaal disclosed the method of claim 11. Yavatkar further disclosing: deriving a set of logical routes from a network topology mapping, wherein each logical route is a series of endpoints that comprise an endpoint-to-endpoint route for completing the requested action (refer to Col 17, Lines 1-10).

13. Referring to Claim 15, Yavatkar, Aoki and Phaal disclosed the method of claim 1. Yavatkar further disclosing displaying the identified source of network packets to the system administrator in real time (refer to Col 1, Lines 10-35 and Col 4, Lines 15-24).

14. Referring to Claim 16, Yavatkar discloses an apparatus for monitoring network packets transmitted within a distributed data processing system, the apparatus comprising: means for

monitoring multiple sources of network packets within the distributed data processing system (refer to Col 4, Lines 1-3, Col 15, Lines 65-66); means for identifying a source of network (refer to abstract); and means for alerting a system administrator to the identified source of network packets by returning packet usage events to the packet usage manager in response to a determination that a packet surpassed a limitation specified by the packet filtering parameters (refer to Col 16, Lines 17-21 and Col 17, Lines 25-30 and Col 18, Lines 10-18 and Col 19, Lines 1-8), wherein the means for identifying comprises: means for deploying distributed packet snoopers from a packet usage manager to monitor the multiple sources of network packets (refer to Col 5, Lines 36-45, Col 15, Lines 35-40); means for receiving packet filtering parameters at each of the deployed distributed packet snoopers, wherein the packet filtering parameters specify at least a packet type and a packet size of a packet (id type of traffic include the packet type and packet size, refer to Col 16, Lines 1-17); and means for matching packet filtering parameters against transmitted packets (refer to Col 15, Lines 16-45).

Although Yavatkar disclosed the invention substantially as claimed, Yavatkar did not explicitly disclosing " identifying a source of network packets as generating network packets having packet size characteristics directly related to packet size of individual packets of the network packets that satisfy one or more predetermined conditions."

Aoki, in analogous art, disclosing "identifying a source of network packets as generating network packets having packet size characteristics directly related to packet size of individual packets of the network packets that satisfy one or more predetermined conditions (refer to Col 7, Lines 25-65)"

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine Yavatkar and Aoki because Aoki's teaching of "identifying a source of network packets as generating network packets having packet size characteristics directly related to packet size of individual packets of the network packets that satisfy one or more predetermined conditions" would improve the Yavatkar's system performance by efficiently calculate the effective bandwidth during the time when the network is congested (also supported by Phaal, refer to par 0031 and 0069).

15. Referring to Claim 17, Yavatkar, Aoki and Phaal disclosed the apparatus of claim 16. Although Yavatkar disclosed the invention substantially as claimed, Yavatkar did not explicitly disclosing "wherein a predetermined condition of the one or more predetermined conditions is a packet size less than a predetermined packet size threshold value."

Aoki, in analogous art, disclosing "wherein a predetermined condition of the one or more predetermined conditions is a packet size less than a predetermined packet size threshold value (refer to Col 7, Lines 25-65)"

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine Yavatkar and Aoki because Aoki's teaching of "wherein a predetermined condition of the one or more predetermined conditions is a packet size less than a predetermined packet size threshold value" would improve the Yavatkar's system performance by efficiently calculate the effective bandwidth during the time when the network is congested (also supported by Phaal, refer to par 0031 and 0069).

16. Referring to Claim 18, Yavatkar, Aoki and Phaal disclosed the apparatus of claim 16. Although Yavatkar disclosed the invention substantially as claimed, Yavatkar did not explicitly disclosing "wherein a predetermined condition of the one or more predetermined conditions is a computed percentage value of an actual packet payload size in comparison to a maximum available packet payload size."

Aoki, in analogous art, disclosing "wherein a predetermined condition of the one or more predetermined conditions is a computed percentage value of an actual packet payload size in comparison to a maximum available packet payload size (refer to Col 11, Lines 35-60)"

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine Yavatkar and Aoki because Aoki's teaching of "wherein a predetermined condition of the one or more predetermined conditions is a computed percentage value of an actual packet payload size in comparison to a maximum available packet payload size" would improve the Yavatkar's system performance by efficiently calculate the effective bandwidth during the time when the network is congested (also supported by Phaal, refer to par 0031 and 0069).

17. Referring to Claim 19, Yavatkar, Aoki and Phaal disclosed the apparatus of claim 16, Yovatkar disclosing wherein a predetermined condition of the one or more predetermined conditions is a count of a number of packets, where the number packets is the number of individual packets having a packet size less than a predetermined packet size threshold value, that exceed a predetermined maximum count threshold value (capable to detect the large amount of packets, refer to Col 13, Lines 20-30 and Col 16, Lines 1-18)

18. Referring to Claim 20, Yavatkar, Aoki and Phaal disclosed the apparatus of claim 16. Yavatkar further discloses wherein a predetermined condition of the one or more predetermined conditions is a computed percentage value of a number of packets, where the number of packets is the number of individual packets having a packet size less than a predetermined packet size threshold value, in comparison to a number of packets from the identified source of network packets (refer to Col 16, Lines 1-18).

19. Referring to Claim 21, Yavatkar, Aoki and Phaal disclosed the apparatus of claim 16. Yavatkar further disclosing: means for halt execution of the identified source in response to a request of the system administrator (refer to Col 9, lines 25-30).

20. Refering to Claim 22, Yavatkar, Aoki and Phaal disclosed the apparatus of claim 16 Yavatkar further discloses further comprising: means for pausing execution of the identified source in response to a request of the system administrator (refer to Col 9, Lines 25-30).

21. Referring to Claim 23, Yavatkar, Aoki and Phaal disclosed the apparatus of claim 16. Yavatkar further discloses comprising: means for initiating a packet snooping session (refer to Col 13, Lines 55-67).

22. Referring to Claim 26, Yavatkar, Aoki and Phaal disclosed the apparatus of claim 16 Yavatkar further discloses: means for receiving a request for an action at a target resource within the distributed data processing system, wherein completion of the action depends upon

operations of a set of resources along a logical route through the distributed data processing system, wherein the request for the action at the target resource is associated with a user or an application.

23. Referring to Claim 27, Yavatkar, Aoki and Phaal disclosed the apparatus of claim 26. Yavatkar further discloses: means for deriving one of the packet filtering parameters from an application or a user associated with the request for the action at the target resource (refer to Col 3, Lines 25-60).

24. Referring to Claim 28, Yavatkar, Aoki and Phaal disclosed the apparatus of claim 26. Yavatkar further discloses: means for selecting by the system administrator one of the packet filtering parameters by choosing among a plurality of active applications or users within the data processing system (refer to Col 11, Lines 50-55).

25. Referring to Claim 29, Yavatkar, Aoki and Phaal disclosed the apparatus of claim 26. Yavatkar further discloses: means for deriving a set of logical routes from a network topology mapping, wherein each logical route is a series of endpoints that comprise an endpoint-to-endpoint route for completing the requested action (refer to Col 17, Lines 1-10).

26. Referring to Claim 30, Yavatkar, Aoki and Phaal disclosed the apparatus of claim 16. Yavatkar further discloses: means for displaying the identified source of network packets to the system administrator in real time (refer to Col 1, Lines 10-35 and Col 4, Lines 15-24).

27. Referring to Claim 31, Aoki discloses computer program product in a computer-readable medium for use within a distributed data processing system for monitoring network packets transmitted within the distributed data processing system, the computer program product comprising: instructions for monitoring multiple sources of network packets within the distributed data processing system (refer to Col 4, Lines 1-3, Col 15, Lines 65-66); instructions for identifying a source of network (refer to abstract); and instructions for alerting a system administrator to the identified source of network packets by returning packet usage events to the packet usage manager in response to a determination that a packet surpassed a limitation specified by the packet filtering parameters (refer to Col 16, Lines 17-21, and Col 17, Lines 25-30 and Col 18, Lines 10-18 and Col 19, Lines 1-7), wherein the instructions for identifying comprises: instructions for deploying distributed packet snoopers from a packet usage manager to monitor the multiple sources of network packets (refer to Col 5, Lines 36-45 and Col 15, Lines 35-40); instructions for receiving packet filtering parameters at each of the deployed distributed packet snoopers, wherein the packet filtering parameters specify at least a packet type and a packet size of a packet (refer to Col 17, Lines 1-17); instructions for matching packet filtering parameters against transmitted packets (refer to Col 15, Lines 16-45).

Although Yavatkar disclosed the invention substantially as claimed, Yavatkar did not explicitly disclosing " identifying a source of network packets as generating network packets having packet size characteristics directly related to packet size of individual packets of the network packets that satisfy one or more predetermined conditions."

Aoki, in analogous art, disclosing "identifying a source of network packets as generating network packets having packet size characteristics directly related to packet size of individual

packets of the network packets that satisfy one or more predetermined conditions (refer to Col 7, Lines 25-65)"

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine Yavatkar and Aoki because Aoki's teaching of "identifying a source of network packets as generating network packets having packet size characteristics directly related to packet size of individual packets of the network packets that satisfy one or more predetermined conditions" would improve the Yavatkar's system performance by efficiently calculate the effective bandwidth during the time when the network is congested (also supported by Phaal, refer to par 0031 and 0069).

28. Referring to Claim 32, Yavatkar, Aoki and Phaal disclosed the computer program product of claim 31. Although Yavatkar disclosed the invention substantially as claimed, Yavatkar did not explicitly disclosing "wherein a predetermined condition of the one or more predetermined conditions is a packet size less than a predetermined packet size threshold value."

Aoki, in analogous art, disclosing "wherein a predetermined condition of the one or more predetermined conditions is a packet size less than a predetermined packet size threshold value (refer to Col 7, Lines 25-65)"

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine Yavatkar and Aoki because Aoki's teaching of "wherein a predetermined condition of the one or more predetermined conditions is a packet size less than a predetermined packet size threshold value" would improve the Yavatkar's system performance by efficiently

calculate the effective bandwidth during the time when the network is congested (also supported by Phaal, refer to par 0031 and 0069).

29. Referring to Claim 33. Yavatkar, Aoki and Phaal disclosed the computer program product of claim 31.

Although Yavatkar disclosed the invention substantially as claimed, Yavatkar did not explicitly disclosing "wherein a predetermined condition of the one or more predetermined conditions is a computed percentage value of an actual packet payload size in comparison to a maximum available packet payload size."

Aoki, in analogous art, disclosing "wherein a predetermined condition of the one or more predetermined conditions is a computed percentage value of an actual packet payload size in comparison to a maximum available packet payload size (refer to Col 11, Lines 35-60)"

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine Yavatkar and Aoki because Aoki's teaching of "wherein a predetermined condition of the one or more predetermined conditions is a computed percentage value of an actual packet payload size in comparison to a maximum available packet payload size" would improve the Yavatkar's system performance by efficiently calculate the effective bandwidth during the time when the network is congested (also supported by Phaal, refer to par 0031 and 0069).

30. Referring to Claim 34, Yavatkar, Aoki and Phaal disclosed the computer program product of claim 31, Yovatkar further discloses wherein a predetermined condition of the one or

more predetermined conditions is a count of a number of packets, where the number of packets is the number of individual packets having a packet size less than a predetermined packet size threshold value, that exceed a predetermined maximum count threshold value (refer to Col 13, Lines 20-30 and Col 16, Lines 1-18).

31. Referring to Claim 35, Yavatkar, Aoki and Phaal disclosed the computer program product of claim 31, Yovatkar further discloses wherein a predetermined condition of the one or more predetermined conditions is a computed percentage value of a number of packets, where the number of packets is the number of individual packets having a packet size less than a predetermined packet size threshold value, in comparison to a number of packets from the identified source of network packets (refer to Col 16, Lines 1-18).

32. Referring to Claim 36, Yavatkar, Aoki and Phaal disclosed the computer program product of claim 31. Yavatkar further discloses: instructions for halting execution of the identified source in response to a request of the system administrator (refer to Col 9, Lines 25-30).

33. Referring to Claim 37, Yavatkar, Aoki and Phaal disclosed the computer program product of claim 31. Yavatkar further discloses instructions for pausing execution of the identified source in response to a request of the system administrator (refer to Col 9, Lines 25-30).

34. Referring to Claim 38, Yavatkar, Aoki and Phaal disclosed the computer program product of claim 31. Yavatkar further discloses: instructions for initiating a packet snooping session (refer to Col 13, Lines 55-67).

35. Referring to Claim 41, Yavatkar, Aoki and Phaal disclosed the computer program product of claim 31. Yavatkar further discloses: instructions for receiving a request for an action at a target resource within the distributed data processing system (refer to Col 7, Lines 42-60), wherein completion of the action depends upon operations of a set of resources along a logical route through the distributed data processing system, wherein the request for the action at the target resource is associated with a user or an application (refer to Fig 3).

36. Referring to Claim 42, Yavatkar, Aoki and Phaal disclosed the computer program product of claim 41. Yavatkar further discloses: instructions for deriving one of the packet filtering parameters from an application or a user associated with the request for the action at the target resource (refer to Col 3, Lines 25-60).

37. Referring to Claim 43, Yavatkar, Aoki and Phaal disclosed the computer program product of claim 41. Yavatkar further discloses: instructions for selecting by the system administrator one of the packet filtering parameters by choosing among a plurality of active applications or users within the data processing system (refer to Col 11, Lines 50-55).

38. Referring to Claim 44, Yavatkar, Aoki and Phaal disclosed the computer program product of claim 41. Yavatkar further discloses: instructions for deriving a set of logical routes from a network topology mapping, wherein each logical route is a series of endpoints that comprise an endpoint-to-endpoint route for completing the requested action (refer to Col 17, Lines 1-10).

39. Referring to Claim 45, Yavatkar, Aoki and Phaal disclosed the computer program product of claim 41. Yavatkar further discloses: instructions for displaying the identified source of network packets to the system administrator in real time (refer to Col 1, Lines 10-35 and Col 4, Lines 15-24).

Conclusion

Examiner's Notes: Examiner has cited particular columns and line numbers in the references applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner. In the case of amending the claimed invention, Applicant is respectfully requested to indicate the portion(s) of the specification which dictate(s) the structure relied on for proper interpretation and also to verify and ascertain the metes and bounds of the claimed invention.

A shortened statutory period for reply to this Office action is set to expire THREE MONTHS from the mailing date of this action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Karen C. Tang whose telephone number is (571)272-3116. The examiner can normally be reached on M-F 7 - 3.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Follansbee can be reached on (571)272-3964. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/K. C. T./

Examiner, Art Unit 2451

/Larry D Donaghue/

Primary Examiner, Art Unit 2454